Инженерный вестник Дона, №6 (2025)
ivdon.ru/ru/magazine/archive/n6y2025/10149

Актуальные виды утечек информации в системе электронного документооборота

И. Л. Панюшкин

Ростовский государственный экономический университет (РИНХ)

Аннотация: Одним из элементов информационной инфраструктуры организации, на который направлена организация комплексной системы защиты конфиденциальной информации, является – система электронного документооборота. Рынок систем электронного документооборота показывает непрерывный рост, благодаря своим преимуществам, что подчеркивает актуальность обеспечения безопасности информации в подобных системах. В статье проведен анализ актуальных видов и каналов утечки информации в системе электронного документооборота.
Ключевые слова: документооборот, конфиденциальность информации, электронный документооборот, система электронного документооборота, утечки информации, актуальные виды утечки информации, информационная безопасность, защита информации, проблемы защиты информации, система защиты информации.

Введение

Организация информационной безопасности (далее ИБ) является актуальным и ключевым вопросом не только для коммерческих организаций, но и для государства, о чем говорит принятие национальной программы «Цифровая экономика Российской Федерации» от 4 июня 2019 года. Особенно значимым этот вопрос становится на фоне роста темпов внедрения технологий и цифровизации экономики, а также роста количества кибератак, которые направлены на причинение коммерческого и репутационного ущерба организации. Все это повышает уровень требований к реализации и обеспечению комплексной системы защиты информации (далее КСЗИ), конфиденциального характера, в организации [1].

Обеспечение ИБ информации, циркулирующей в организации, предполагает под собой соблюдение трех основных принципов защиты информации – конфиденциальность, целостность, доступность [2]. Для этого применяется комплекс мер, который включается в себя правовую, организационную и программно-аппаратную защиту. Главная задача, на

которую направлено соблюдение обозначенных принципов и выделенного комплекса мер – создать условия, в которых будет обеспечено нормальное функционирование информационных ресурсов организации, а также будет обеспечиваться полная защита конфиденциальной информации, которая может лишить организацию конкурентного преимущества [3].

КСЗИ нацелена на организацию защиты таких элементов, как объекты поддерживающей информационной инфраструктуры, объекты автоматизированных систем управления и информационных систем, системы электронного документооборота [4].

В рамках научного исследования была проведена оценка актуальных видов утечек информации для системы электронного документооборота (далее СЭД).

Анализ актуальных утечек информации в системе электронного документооборота

Рынок систем электронного документооборота показывает непрерывный рост. Так, по состоянию на 2024 год, он вырос по отношению к 2023 году на 15% [5]. А если посмотреть на последние 7 лет, начиная с 2018 года, рост интереса организаций к СЭД вырос в 5 раз [6]. Данный рост обуславливается тем, что СЭД помогают компаниям оптимизировать и экономить как временные, так и человеческие ресурсы, которые необходимы для работы с постоянно растущим объемом документов [7]; оптимизировать процессы обработки, хранения, передачи документов; ускорить обмен документами с другими подразделениями, а также партнерами и исполнителями; хранить историю работы с конфиденциальными документами. Приведенные показатели роста и выделенные основные преимущества, еще раз подчеркивают актуальность обеспечения защиты информации, циркулирующей в СЭД [8].

Вопрос организации системы защиты порождает вопрос определения актуальных утечек информации для СЭД организации. Для этого обратимся к статистике российского информационного портала InfoWatch [9]. Из наиболее актуальных данных для сравнения доступны первое полугодие (далее 1Н) 2024 года и 1Н 2023 года.

Начнем рассмотрение актуальных видов утечек информации с распределения утечек по типу умысла (рис.1). Как можно увидеть, в сравниваемых периодах, данные информации об утечках по типу умысла остаются практически неизменными – подавляющее преимущество принадлежит умышленным нарушениям.

Далее обратим внимание на количество утечек информации (рис.2). Как показывает статистика, по отношению к 2023 году, в 2024 году количество утечек информации выросло на 10% - 377 и 415 соответственно. Для полноты картины информационный ресурс приводит данные, начиная с 2022 года, включая и I и II полугодие из доступной информации.

Рис. 1. – Распределение утечек по типу умысла

По количеству утекших данные первое место занимают – персональные данные (далее ПДн) (рис.3). Так, за первые полгода 2024 года их количество составило 989 млн. записей, что на 34% больше аналогичного

периода 2023 года – 737 млн. записей. Однако, здесь стоит отметить, что больше половины записей первого полугодия 2024 г. утекли в рамках одного инцидента, произошедшего 26.02.2024 г. В этот день Роскомнадзор заявил об атаке на их ресурсы, в рамках которой злоумышленниками был скомпилирован и опубликован файл, содержащий 500 млн. записей персональных данных россиян.

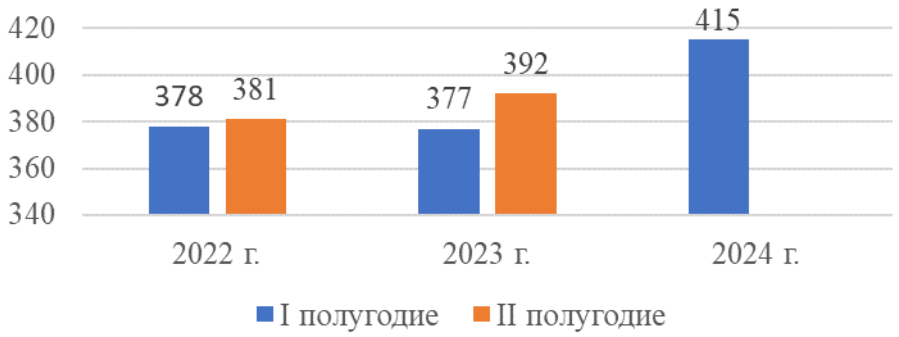

Рис. 2. – Количество утечек информации

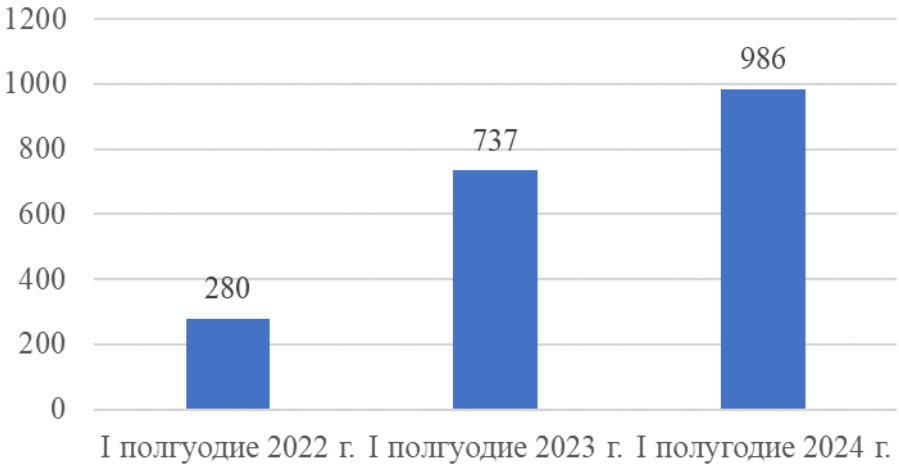

Рис. 3. – Количество утекших записей ПДн, в миллионах

Далее была проанализирована статистика утечек по типам данных (рис.4). 76,1% из всех типов данных занимают персональные данные. Также стоит отметить рост доли утечек информации, содержащей государственную тайну – 11,1% в первом полугодии 2024 года и 6,4% за этот же период 2023 года. По оценкам экспертов, этот рост обусловлен проведением специальной

военной операции (СВО), в рамках которой периодически выявляют лиц, передающих военные данные противнику.

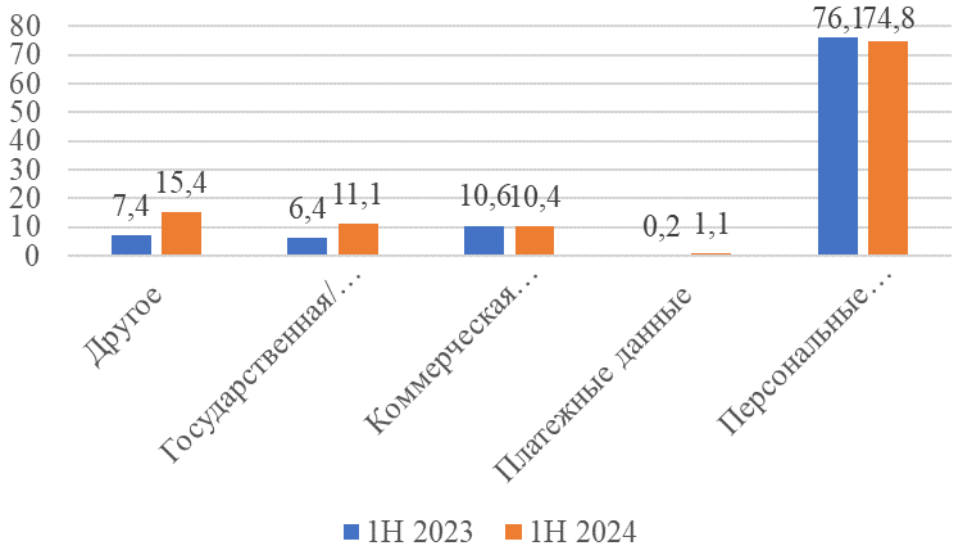

Рис. 4. – Распределение утечек по типам данных, в процентах

Главные виновники совершения атак на информационную безопасность организации, как и в первом полугодии 2023 г., так и в этот же период 2024 г. – внешние нарушители (80,4% и 84,6% соответственно) (рис.5). Также, чаще других, виновниками утечек информации становятся сотрудники организации, хоть и в 1Н 2024 г. году их доля заметно снизилась по отношению к 1Н 2023 г. – 11,8% и 18% соответственно. Однако, аналитики допускают в этих данных погрешность, так как довольно часто инциденты о нарушении безопасности информации оглашаются после длительных разбирательств, либо же не оглашаются вовсе, в целях сохранения репутации и информации о возможных уязвимостях.

Далее обратимся к статистике информационно-аналитического центра Anti-Malware, которую подготовила экспертная группа компании «Солар». Согласно ей – 1/3 утечек информации за 2024 года происходила через мессенджеры (35%). Второе место по количеству занимает электронная почта – 23%. Как отметили эксперты, это два основных канала связи,

применяемые в деловом мире общения и обмена документами, в том числе содержащими конфиденциальную информацию. Также каналами утечки такой информации становились: открытые источники и облачные хранилища – 15%; носители информации – 12%; демонстрация экрана во время конференций – 12%, печать бумажных носителей информации – 3%. [10]

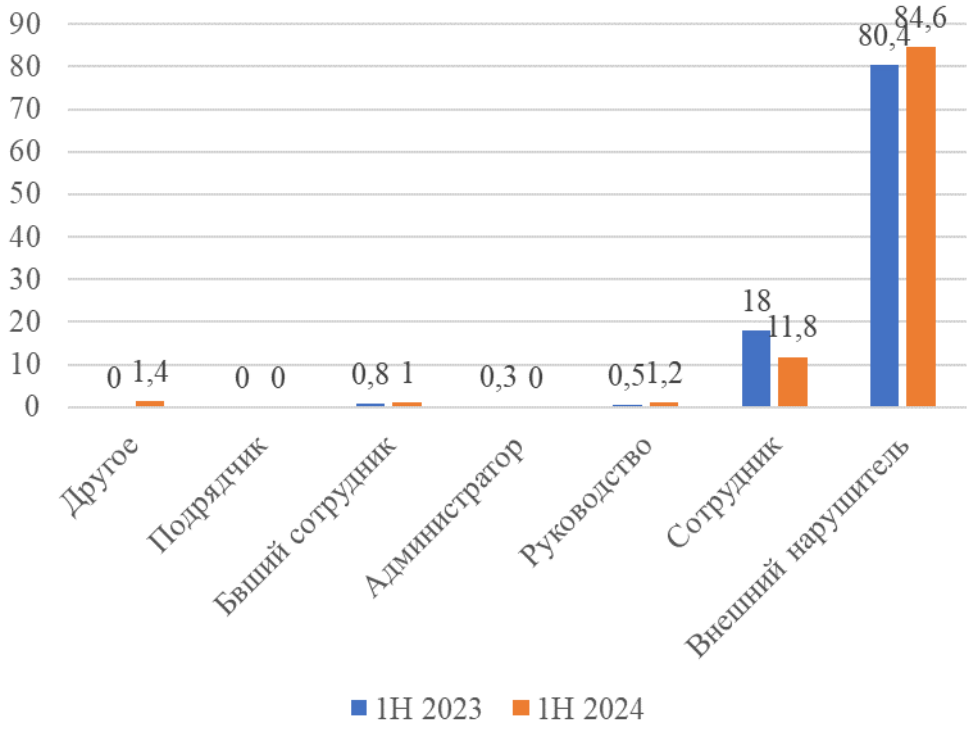

Рис. 5. – Виновники утечек информации, в процентах

Заключение

Как можно заметить, атакам злоумышленников часто подвергаются те типы данных и каналы утечек информации, которые задействованы в СЭД. В свою очередь, сами СЭД могут быть подвержены таким угрозам, как несанкционированный доступ к информации, умышленные или непреднамеренные ошибки в работе сотрудников и руководителей, умышленное повреждение или уничтожение средств защиты, а также коммерческий интерес от продажи конфиденциальной информации. Именно

поэтому важно обеспечивать комплексную систему защиты конфиденциальной информации в системах электронного документооборота, чтобы сохранить как коммерческое преимущество организаций, так и их репутацию.

Литература

1. Мирошниченко М.А., Бондаренко А.А., Пиналова Е.В. Актуальные проблемы обеспечения информационной безопасности систем электронного документооборота в рамках цифровой трансформации // Вестник Академии знаний. 2020. №1 (36). URL: cyberleninka.ru/article/n/aktualnye-problemy-obespecheniya-informatsionnoy-bezopasnosti-sistem-elektron-nogo-dokumentoo-borota-v-ramkah-tsifrovoy

2. Информационная безопасность документооборота // SearchInform. Information Security URL: searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionna%20ya-bezopasnost-dokumentooborota/

3. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона, 2022, № 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010

4. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона, 2019, № 3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859

5. Королев И.Д. Актуальные проблемы разработки, внедрения и применения систем электронного документооборота в действующих и перспективных автоматизированных системах, обрабатывающих конфиденциальную информацию // Молодой ученый. 2018. № 13 (199). URL: moluch.ru/archive/199/49026/

6. Кононок К.А. Анализ и выявление недостатков при работе в системе электронного конфиденциального документооборота // Молодой ученый. 2021. № 52 (394). URL: moluch.ru/archive/394/87343/

7. Kettunen, P., Kallio, J. The Role of Electronic Document Management Systems in the Digital Transformation of Business // International Journal of Information Management. URL: sciencedirect.com/science/article/pii/S0268401219305297

8. Vasileva M., Stoyanov S. Security Challenges of Electronic Document Management Systems: A Review // Journal of Cyber Security Technology/ URL: tandfonline.com/doi/full/10.1080/23742917.2020.1817985

9. Утечки информации в мире и России за первое полугодие 2024 года // InfoWatch URL: infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-i-rossii-za-pervoye-polugo-diye-dve-tysyachi-dvadtsat-chetvertogo-goda.pdf

10. Треть утечек в 2024 году происходили через мессенджеры // Anti-Malware URL: anti-malware.ru/news/2025-02-20-121598/45334

References

1. Miroshnichenko M A., Bondarenko A A., Pinalova E V. Vestnik Akademii znanij. 2020. №1 (36). URL: cyberleninka.ru/article/n/aktualnye-problemy-obespecheniya-informatsionnoy-bezopasnosti-sistem-elektronnogo-dokumentoo-borota-v-ramkah-tsifrovoy

2. Informacionnaya bezopasnost` dokumentooborota [Information security of document management]. SearchInform. Information Security. URL: searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionna%20ya-bezopasnost-dokumentooborota/

3. Ibragimova Z.M., Batchaeva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona, 2022, No. 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010

4. Mentsiev A.U., Chebieva H.S. Inzhenernyj vestnik Dona, 2019, No. 3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859

5. Korolev I.D. Molodoj ucheny`j. 2018. № 13 (199). URL: moluch.ru/archive/199/49026/

6. Kononok K.A. Molodoj ucheny`j. 2021. № 52 (394). URL: moluch.ru/archive/394/87343/

7. Kettunen, P., Kallio, J. International Journal of Information Management. URL: sciencedirect.com/science/article/pii/S026840-1219305297

8. Vasileva M., Stoyanov S. Journal of Cyber Security Technology. URL: tandfonline.com/doi/full/10.1080/23742917 .2020.1817985

9. Utechki informacii v mire i Rossii za pervoe polugodie 2024 goda [Information leaks in the world and Russia for the first half of 2024]. URL: infowatch.ru/sites/default/files/analytics/files/utechki-informa-tsii-v-mire-i-rossii-za-pervoye-polugodiye-dve-tysyachi-dvadtsat-chetvertogo-goda.pdf

10. Tret` utechek v 2024 godu proisxodili cherez messendzhery. [A third of leaks in 2024 occurred through messengers]. URL: anti-malware.ru/news/2025-02-20-121598/45334

Дата поступления: 10.04.2025

Дата публикации: 25.05.2025